Exhibit 22

QUARLES & BRADY LLP
Firm State Bar No. 00443100
Renaissance One, Two N. Central
Phoenix, AZ 85004-2391, 602-229-5200
Brian A. Howie (AZ No. 026021)
Brian.Howie@quarles.com
Lauren E. Stine (AZ No. 025086)
Lauren.Stine@quarles.com
Attorneys for Plaintiffs

SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
2099 Pennsylvania Ave., NW, Ste. 100
Washington, DC 20006, 201-747-1900
Thomas J. Dillickrath* (DC 483710)
TDillickrath@sheppardmullin.com

Four Embarcadero Center, 17th Floor
San Francisco, CA 94111, 415-434-9100
Amar S. Naik* (CA 307208)
ANaik@sheppardmullin.com
Molly C. Lorenzi* (CA 315147)
MLorenzi@sheppardmullin.com

GIBBS & BRUNS LLP
1100 Louisiana, Ste. 5300
Houston, TX 77002, 713-650-8805
Aundrea K. Gulley* (TX 24034468)
agulley@gibbsbruns.com
Denise Drake* (TX 24092358)
DDrake@gibbsbruns.com
Attorneys for The Reynolds and Reynolds Co.

MAYER BROWN LLP
71 S. Wacker Drive
Chicago, IL 60606
312-782-0600
Britt M. Miller* (IL 6256398)
BMiller@mayerbrown.com
Michael A. Scodro* (IL 6243845)
MScodro@mayerbrown.com
Brett E. Legner* (IL 6256268)
BLegner@mayerbrown.com

1999 K Street, NW
Washington, DC 20006
202-263-3000
Mark W. Ryan** (DC 359098)
mryan@mayerbrown.com
Andrew E. Tauber** (DC 495980)
atauber@mayerbrown.com
Attorneys for CDK Global, LLC
**Admitted Pro Hac Vice*
***Pro Hac Vice Forthcoming*

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

CDK Global, LLC, a limited liability company, and The Reynolds and Reynolds Company, a corporation,

Plaintiffs,

vs.

Mark Brnovich, Attorney General of the State of Arizona, and John S. Halikowski, Director of the Arizona Department of Transportation,

Defendants.

Case No. 2:19-CV-04849-GMS

PLAINTIFFS' CONSOLIDATED RESPONSE TO STATE DEFENDANTS' [ECF 40] AND INTERVENOR-DEFENDANT'S [ECF 39] MOTIONS TO DISMISS

(Oral Argument Requested)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES & CONSTITUTIONAL AUTHORITIES

OTHER AUTHORITIES

The motions to dismiss filed by the State Defendants (Mark Brnovich, Attorney General of the State of Arizona, and John Halikowski, Director of the Department of Transportation) and Intervenor-Defendant Arizona Automobile Dealers Association (collectively, the "Defendants") fail on multiple grounds. They ignore and contradict the Complaint's well-pleaded facts, misconstrue the legal standard applicable to Plaintiffs' constitutional claims, and mischaracterize the statutes underlying Plaintiffs' preemption claims. With no basis in law, and a premature reliance on factual disputes, the motions should be denied.

BACKGROUND

Plaintiffs develop, own, operate, and license complex proprietary computer systems known as dealer management systems ("DMSs") that automotive dealerships use to manage their business operations. Compl. ¶¶ 8, 34. Plaintiffs' systems incorporate their respective patents, copyrights, trade secrets, and other intellectual property, including the end-user application software installed on a dealership's PCs, sophisticated network architecture between servers, data centers, and other system components, and proprietary processes for handling data communications between dealers, car manufacturers, and other third parties. *Id.* ¶¶ 8, 12, 34, 39–41, 44–45, 48–49, 71. As part of their DMSs, Plaintiffs deploy proprietary interfaces to handle automated data communications between dealers, car manufacturers, application providers, credit bureaus, and other third parties approved by Plaintiffs. *Id.* ¶¶ 12, 96. It is impossible for any person to access, use, or modify Plaintiffs' DMSs or the databases therein without running or leveraging copyrighted software programs. *Id.* ¶¶ 15, 49, 96, 122.

Plaintiffs' licensing agreements with dealers contain detailed provisions setting forth Plaintiffs' exclusive rights to control access to their respective systems. *Id.* ¶¶ 50, 84–94. Per these agreements, dealerships access the DMS through nontransferable login credentials meant only for dealership employees and "agree not to connect any third-party software" to their DMS. *Id.* ¶¶ 36, 50, 95. To help dealers retrieve their information from these systems, Plaintiffs have developed methods to permit dealers to access their data and send just that

data to third parties of the dealers' choosing at no charge. *Id.* ¶¶ 100–01, 107. At the same time, Plaintiffs also have developed programs that allow third parties to engage in cooperative engineering, providing those parties with safe, controlled access to data housed in the systems as an alternative method for dealers to send their data to these third parties. *Id.* ¶¶ 97–99, 103–06. Plaintiffs must approve those third parties, who then enter into cooperative agreements with Plaintiffs. *Id.*

Because Plaintiffs' DMSs store and process sensitive consumer, financial, and proprietary data, they must securely manage the flow of such information between dealers and other third parties involved in a dealer's business operations. *Id.* ¶¶ 9, 28, 34, 42, 46. Plaintiffs employ a number of technological countermeasures to protect the data and their systems by implementing strict access controls against unauthorized access. *Id.* ¶¶ 51–67. These features include password protections, CAPTCHA prompts, and other security protocols preventing unauthorized, automated access to the DMS. *Id.* ¶¶ 51–57, 61–64. These security controls are critical to ensuring that Plaintiffs meet their statutory and contractual obligations to secure the data stored and processed on their DMSs. *Id.* ¶ 68.

Unhappy with the terms of their freely negotiated contracts with Plaintiffs, the dealers spearheaded a legislative effort to rewrite the terms of those deals. *Id.* ¶¶ 2–3, 127, 143. They succeeded: The legislature passed the DMS Law that Plaintiffs challenge here. *Id.* ¶¶ 1, 159. But that law recklessly and dangerously rewrites those private contracts, takes Plaintiffs' ability to control access to their computer systems, and requires Plaintiffs to tear down their data security protections. *Id.* ¶¶ 13–14, 127, 131–33, 138, 140–43.

The DMS Law thus threatens Plaintiffs' intellectual property rights and conflicts with Plaintiffs' legal obligations by requiring Plaintiffs to give third parties unfettered access to their respective systems and the data these systems store and process. *Id.* ¶¶ 1, 126, 141. The DMS Law effectively requires Plaintiffs to "tear down their security walls and build a back door to Plaintiffs' DMS, giving data pirates and cyberthieves free license to jump unimpeded into the pool of data provided by Arizona consumers." *Id.* ¶ 17; *see also id.* ¶¶ 13, 19, 66, 108, 110, 114, 116–19, 120–25. The DMS Law prohibits a DMS provider

from taking "any action by contract, technical means or otherwise" to prohibit or limit the copying, sharing or use of such data. *Id.* ¶ 131. Further, the DMS Law forbids Plaintiffs from placing any restriction on data extractors—entities with whom Plaintiffs have no contractual relation and that have historically violated federal criminal law—from accessing Plaintiffs' systems, copying Plaintiffs' software and code, and extracting or modifying the data stored or processed on Plaintiffs' systems. *Id.* ¶¶ 49, 109–13, 132–33.

The DMS Law declares the use of system-access controls and encryption to be "cyber ransom." *Id.* ¶¶ 138, 142, 147. Defining "protected dealer data" to include any data "that relates to a dealer's business operations," the DMS Law would require Plaintiffs to give third parties free access to Plaintiffs' intellectual property and to licensed data subject to strict use and sharing restrictions. *Id.* ¶ 111.

To comply with the DMS Law, Plaintiffs must write new computer code and supporting materials that disable the security protocols embedded in their system and reengineer the system functionality of data communication tools and system interfaces. *Id.* ¶¶ 15, 19, 20, 142–43. It eviscerates Plaintiffs' ownership rights in their systems and conflicts with federal law. *Id.* ¶¶ 108, 135–38, 144, 161, 237–39.

ARGUMENT

I. Plaintiffs' Claims Are Ripe.

Citing three factors courts consider when evaluating ripeness (ECF 40 at 5–6),[1] Defendants argue that Plaintiffs' claims are not ripe because Plaintiffs do not allege (1) "that they actually plan to do any of [the] activities" made criminal by the DMS Law, (2) "that any Defendant has communicated a specific warning or threat to prosecute" Plaintiffs, or (3) "that there is a history of past prosecution under the [DMS] Law." *Id.* at 6. But Defendants misread both the Complaint and established law, which is inconsistent with Defendants' impossibly narrow view of what Plaintiffs must do to state a ripe claim.[2]

[1] Citations to ECF documents refer to the party's original pagination.

[2] This is particularly so where, as here, the plaintiff raises a First Amendment claim, and Article III's case-or-controversy requirements are at their most relaxed. *Ariz. Right to Life Political Action Comm. v. Bayless*, 320 F.3d 1002, 1006 (9th Cir. 2003).

Contrary to Defendants' contention, Plaintiffs need not specifically vow to commit criminal acts in the future. Plaintiffs allege that the DMS Law criminalizes their current and longstanding business practices, as set forth in their existing contracts with dealers and as required by federal law. Compl. ¶¶ 138, 142–43, 171–74, 237–39. Thus, Plaintiffs allege they would need to change their current conduct to comply with the law—which is more than enough to plead a ripe cause of action. *Stormans, Inc. v. Selecky*, 586 F.3d 1109, 1123 (9th Cir. 2009) (claim ripe where plaintiff's historical conduct would violate the challenged rule).

Plaintiffs' fear of prosecution is genuine, not "imaginary or wholly speculative." *Babbitt v. United Farm Workers Nat'l Union*, 442 U.S. 289, 302 (1979). Indeed, Plaintiffs are able to lawfully continue their existing practices for now only because the State Defendants agreed to temporarily stay enforcement of the DMS Law. ECF 29. Plaintiffs allege that the law was passed to change their business practices in particular. Compl. ¶¶ 3, 142–43. Because "the plain purpose of the legislation [is] to proscribe" Plaintiffs' conduct, their claims are ripe. *Frazier v. Boomsma*, 2007 WL 2808559, at *8 (D. Ariz. 2007).

Here, there is no need for the government to make overt threats of enforcement to create a live case or controversy. It is sufficient that the government has not disavowed (other than temporarily) its willingness to prosecute Plaintiffs, even in the State Defendants' Motion to Dismiss. *Babbitt*, 442 U.S. at 302 ("the State has not disavowed any intention of invoking the criminal penalty"); *Ariz. Right to Life Political Action Comm.*, 320 F.3d at 1006 ("Arizona has not suggested that the legislation will not be enforced if [the plaintiff] … were to violate its provisions…."). And it is nonsensical for Defendants to require a history of enforcement under the DMS Law where, as here, Plaintiffs brought suit, and entered into an agreed stay of enforcement, before the law even went into effect.

Nor is there any merit in Defendants' assertion that "hypothetical factual questions and hypothetical legal interpretations" defeat ripeness. ECF 40 at 6. The Complaint details a live, concrete controversy. It explains that the DMS Law is designed to change Plaintiffs' existing business practices and subjects them to criminal liability if they fail to do so. Thus,

contrary to Defendants' suggestion, this case is unlike *National Park Hospitality Association v. Department of the Interior*, 538 U.S. 803 (2003), which involved an abstract dispute over a general statement of agency policy with no certain effect on the plaintiff's conduct. Here, the DMS Law requires Plaintiffs to change their conduct immediately or face criminal prosecution. Accordingly, this case presents a ripe controversy.

II. Defendants Offer No Basis To Dismiss Plaintiffs' Preemption Claims.

A. The Governing Standard.

Indirectly quoting *United States v. Salerno*, 481 U.S. 739 (1987), Defendants suggest (*see* ECF 39 at 6) that the DMS Law is not preempted unless "no set of circumstances exists under which the Act would be valid." 481 U.S. at 745. But even if that "dictum," *City of Chicago v. Morales*, 527 U.S. 41, 55 n.22 (1999), provides the applicable standard, Plaintiffs have alleged sufficient facts to satisfy it.

For example, because the CFAA declares that access to a protected computer may be authorized only by the owner of the computer and the Complaint alleges that Plaintiffs own the servers on which their DMSs operate (*see, e.g.*, Compl. ¶¶ 24, 27, 34), there is no set of circumstances in which the DMS Law, which grants dealers the power to authorize access to Plaintiffs' DMSs, could be valid. Similarly, because the DMCA gives copyright owners the exclusive right to electronically control access to their works and the Complaint alleges that Plaintiffs hold copyrights in material on their DMSs (*see, e.g.*, Compl. ¶¶ 8, 34, 39, 42, 48–49), there is no set of circumstances in which the DMS Law, which gives dealers the power to authorize third-party access to Plaintiffs' copyrighted works, could be valid.

Notably, Defendants do not identify any application of the DMS Law that would be permissible under the CFAA, the DMCA, or the other federal statutes raised in the Complaint. But even if Defendants could "point to a non-preempted application of the law," that "is not dispositive." *Backpage.com, LLC v. McKenna*, 881 F. Supp. 2d 1262, 1274 (W.D. Wash. 2012). "The Ninth Circuit clarified how *Salerno* is to be applied in *United States v. Arizona*." *Id.* In that case, in which the federal government brought a pre-enforcement preemption challenge to an Arizona state law, the Ninth Circuit

> stress[ed] that the question before us is not, as Arizona has portrayed, whether state and local law enforcement officials can *apply* the statute in a constitutional way. Arizona's framing of the *Salerno* issue assumes that [the state statute] is not preempted on its face, and then points out allegedly permissible applications of it. This formulation misses the point: there can be no constitutional application of a statute that, on its face, conflicts with Congressional intent and therefore is preempted by the Supremacy Clause.

United States v. Arizona, 641 F.3d 339, 346 (9th Cir. 2011), *aff'd in part, rev'd in part and remanded on other grounds*, 567 U.S. 387 (2012) ("*Arizona*"). Having found that the state statute "facially conflict[ed] with Congressional intent," the analysis was complete; only "[i]f that were not the case" would the court "have next considered whether the statute could be applied in a constitutional manner." *Id.* at 346 n.4. In other words, a court applying *Salerno* must first determine whether the state law at issue conflicts with congressional intent; only if it does not does the court ask whether the state law may be applied in certain circumstances. Here, because the DMS Law conflicts with congressional intent for the reasons detailed below (*see infra* at 7–21), it is impliedly preempted under *Salerno*.[3]

[3] Although Plaintiffs' preemption claims are not subject to dismissal under *Salerno*, Plaintiffs dispute *Salerno*'s applicability to those claims. While the Ninth Circuit has "chosen to continue applying *Salerno*," it acknowledges that "*Salerno*'s applicability in preemption cases is not entirely clear." *Puente Ariz. v. Arpaio*, 821 F.3d 1098, 1104 (9th Cir. 2016). In particular, the Ninth Circuit recognizes that because "[t]he Supreme Court's majority opinion in *Arizona* does not cite *Salerno*," some courts, including the Third Circuit, have "conclude[d] *Salerno* does not apply to facial preemption challenges." *Id.* at 1104 n.6 (citing *Lozano v. City of Hazleton*, 724 F.3d 297, 313 n.22 (3d Cir. 2013)). Indeed, even before *Arizona*, the Supreme Court questioned the applicability of the *Salerno* "dictum." *Morales*, 527 U.S. at 55 n.22. Noting that "[t]he *Salerno* formulation … has been criticized and questioned by the Supreme Court," one district court within the Ninth Circuit has thus rejected the proposition that *Salerno* "is applicable to facial challenges to a *state* law based on a theory of conflict preemption." *Rocky Mountain Farmers Union v. Goldstene*, 843 F. Supp. 2d 1042, 1066–67 (E.D. Cal. 2011), *aff'd in part, rev'd in part, and vacated on other grounds sub nom. Rocky Mountain Farmers Union v. Corey*, 730 F.3d 1070 (9th Cir. 2013). And in at least one case, the Ninth Circuit has concluded that a district court's "reli[ance] upon the standard of review in … *Salerno* … was incorrect." *Planned Parenthood of S. Ariz. v. Lawall*, 307 F.3d 783, 786 n.1 (9th Cir. 2002). A literal application of *Salerno*'s "no set of circumstances" formulation makes no sense where, as here, a state law is challenged as impliedly preempted because it "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." *Hines v. Davidowitz*, 312 U.S. 52, 67 (1941). Because a state law must yield to federal law when it impedes "the *full* purposes and objectives of Congress," *id.* (emphasis added), pleading facts that, if true,

B. Plaintiffs' CFAA Claim Is Not Subject To Dismissal.

Defendants do not dispute that the CFAA makes it illegal for anyone to access a computer "'without authorization'" and thereby "'obtain[] … information from any protected computer." ECF 39 at 8 (quoting 18 U.S.C. § 1030(a)(2)). Nor do Defendants dispute that Plaintiffs' DMSs are "protected computers" within the meaning of the CFAA (Compl. ¶ 203 (citing 18 U.S.C. § 1030(e)(1)) or deny that third-party integrators "obtain[] … information" from Plaintiffs' DMSs when they access those systems (*see* Compl. ¶¶ 109, 111–13, 117, 119). Despite all this, Defendants still argue that "there is no conflict" between the DMS Law and the CFAA because the DMS law "requires DMS providers to provide data access only to users with express written authorization of the dealers." ECF 39 at 8. Defendants' argument rests on a fundamental misunderstanding of the CFAA.

That a dealer might grant a so-called third-party integrator permission to access the dealer's data is irrelevant. Plaintiffs, not dealers, own Plaintiffs' DMSs. Compl. ¶¶ 8, 12–13. Accordingly, only Plaintiffs can authorize access to their DMSs. As a federal court applying the CFAA specifically to DMSs held, "the 'authorization' required for lawful access under the CFAA must come from *the owner of the computer system*, not from anyone who happens to use the system." *In re Dealer Mgmt. Sys. Antitrust Litig.*, 362 F. Supp. 3d 558, 570 (N.D. Ill. 2019) (citing Oral Arg. Tr. 51 (Easterbrook, J.), *Authenticom, Inc. v. CDK Glob., LLC*, 874 F.3d 1019 (7th Cir. 2017) (Nos. 17-2540, -2541)) (emphasis added).

Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016), confirms that under the CFAA "authorization" must come from the owner of the computer system. In that case, the defendant website created a link on its home page that, when clicked, caused messages to be sent through its users' Facebook accounts. *Id.* at 1063. Facebook sued under the CFAA and won. *Id.* at 1065–69. Rejecting the defendant's argument that it was authorized to access Facebook's computers under the CFAA because the individual Facebook users had granted the defendant permission to access their accounts, the Ninth Circuit held that "[t]he consent that [defendant] had received from Facebook users was not

---

would establish *any* interference with Congress's goals is sufficient to avoid dismissal.

sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission." *Id.* at 1068. In short, the CFAA prohibited authorized Facebook users from granting third-party access to Facebook's computers without Facebook's consent. Or as the court held elsewhere, the CFAA grants computer owners "exclusive discretion" to determine who is authorized to access their computers. *United States v. Nosal*, 844 F.3d 1024, 1036 (9th Cir. 2016) ("*Nosal II*").[4] Thus, the Ninth Circuit's "position [is] that authorization can be given only by the system owner." *Id.* at 1052 (Reinhardt, J., dissenting).

Notwithstanding this binding precedent, Defendants argue that the CFAA is "analogous" to laws prohibiting burglary and trespass, which apply only to those who are "'not … authorized'" to "'enter[] or remain[] on'" the property in question. ECF 39 at 8 n.9 (quoting A.R.S. § 13-1501(2)). That is true, but it does not help Defendants. Consider, for example, a consignment shop. The fact that the shop is storing an item that has been consigned for sale does not give the item's owner the power to authorize a third party to enter the premises without the shop owner's permission. If a third party entered the shop without permission of its owner, that party would be guilty of burglary or trespassing, even if the item's owner purported to authorize the entry.

Nor does this construction of the CFAA "criminalize dealers granting access to their own data." ECF 39 at 9. What the CFAA prohibits is enabling third parties to gain access to a protected computer without the permission of the system owner. For purposes of the CFAA, who owns the data stored on the computer is irrelevant. Take, for example, an article published in the *Yale Law Journal* and available on Westlaw. Although it has contracted with Westlaw to make its articles available to Westlaw subscribers, the journal owns the copyright in such articles. There is no question that as the copyright owner the journal may provide copies of its articles to anyone it chooses. And each editor of the journal, like every

[4] Defendants cite (ECF 39 at 9) *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) ("*Nosal I*"), an earlier decision in the same matter, but it is inapposite. It addressed whether someone who has authorization to access a computer system violates the CFAA by "exceed[ing]" his or her "authorized access." 18 U.S.C. § 1030(a)(2). It did not address who has the power to authorize access to a computer system in the first place—the issue here.

law student in the country, has a password-protected Westlaw account. But neither fact entitles the journal or its editors to give a third party access to Westlaw's proprietary system to download a *Yale Law Journal* article. So too here. Dealers may give anyone they wish their data (subject to privacy laws and contractual obligations), but they may not give a third party access to Plaintiffs' DMSs, even if that party would use such access to obtain only the dealer's data.

Defendants' reliance (ECF 39 at 9) on *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099 (N.D. Cal. 2017), *aff'd*, 938 F.3d 985 (9th Cir. 2019), is misplaced. In fact, *hiQ* supports Plaintiffs' contention that the CFAA preempts the DMS Law and confirms that anyone attempting to access a DMS or other computer system must receive authorization from the system's owner. As the court noted, "[c]ontext matters." *Id.* at 1112. The result in *hiQ* turned on the fact that the defendant accessed "a publicly viewable web page open to all on the Internet." *Id.* According to both the trial court and the Ninth Circuit, that fact distinguished *hiQ* from both *Facebook*, where "the defendants had bypassed a password authentication system," and *Nosal*, where the defendant had accessed "*private* data protected by an authentication process." *Id.*; *see also hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1001–03 (9th Cir. 2019). And it distinguishes *hiQ* from this case, where Plaintiffs employ various technological measures to control access to their DMSs, which contain proprietary and other non-public information. Compl. ¶¶ 39, 42, 51–68.[5]

Nor is there merit to the argument that the CFAA and DMS Law are not "in conflict" but instead "work in tandem." ECF 39 at 10. While the DMS Law might require Plaintiffs to grant access to their DMSs only to "third parties that have met STAR Standards" (*id.*), that limitation does not obviate the conflict between the DMS Law, which purports to grant dealers control over who may access Plaintiffs' DMSs, and the CFAA, which grants

[5] Ignoring the Complaint's well-pleaded allegations, Defendants imply that the dealers' "own data" is the only information that third-party integrators could obtain once inside the DMSs. ECF 39 at 9–11. But, as Plaintiffs allege, "DMSs house both 'protected dealer data' as defined by the DMS Law and other proprietary data, including Plaintiffs' intellectual property and data licensed to Plaintiffs by OEMs and other parties." Compl. ¶ 111; *see also id.* ¶¶ 8, 113. Providing third parties access to the DMSs as mandated by the DMS Law would give them access "to that other proprietary data as well." *Id.* ¶ 111.

Plaintiffs "exclusive discretion" to determine who is authorized to access their computers. *Nosal II*, 844 F.3d at 1036; *accord Facebook*, 844 F.3d at 1063; *In re Dealer Mgmt. Sys. Antitrust Litig.*, 362 F. Supp. 3d at 570.

Disregarding A.R.S. § 28-4653, which compels DMS providers to grant dealer-designated third parties access to their systems, Defendants suggest that the DMS Law does not conflict with the CFAA because A.R.S. § 28-4652 "provides an alternative to 'access to the [DMS]' by permitting pushing data through 'any widely acceptable electronic file format' that … meets the STAR Standards." ECF 39 at 10. But § 28-4652 does not cure the fatal flaws of § 28-4653. It declares that "a manufacturer or a third party"—defined to include a DMS provider, A.R.S. § 28-4651(10)(a)—"may not require *a dealer* to grant the manufacturer [or] the third party … access *to the dealer's dealer data system*," and that "[i]nstead of providing a manufacturer or third party with access to the dealer's data system, *a dealer* may submit or push data or information to a manufacturer or third party through any widely acceptable electronic file format or protocol that complies with the star standards." A.R.S. § 28-4652 (emphasis added). Thus, it gives *dealers* an option on how they provide their data to DMS providers but does not give DMS providers an option on how they receive dealer data. Nor does it prevent dealer-designated third parties from accessing DMSs to extract data, as integrators do, without the owners' permission. Compl. ¶¶ 109, 113.

Defendants also misread the DMS Law when, citing A.R.S. § 28-4654, they say that "Plaintiffs can comply with the Law … by creating an API"— Application Programming Interface—"between the dealer's DMS database and a database outside the DMS, requiring no third-party access to the DMS at all." ECF 39 at 10. As an initial matter, Defendants are wrong to say that use of an API involves "no third-party access to the DMS."[6] Further,

[6] Whether one can transfer data using an API without "access to the DMS," as Defendants assert, is a factual question not susceptible to resolution on a motion to dismiss. And the assertion is contrary to the Complaint's well-pleaded allegations. For example, Plaintiffs allege that Reynolds' "DMS is an integrated system of hardware and software components" that "include[s]" the "secured interfaces between [Reynolds'] servers and the dealer's computers." Compl. ¶ 44.

whether Plaintiffs can comply with the DMS Law is irrelevant: the question here is whether the DMS Law is an obstacle to Congress's goal in enacting the CFAA, not whether compliance with DMS Law is impossible. Regardless, providing third-party integrators with access via APIs would not satisfy Plaintiffs' obligation under the provision Defendants cite. The provision declares that DMS providers "shall" do two things: "[p]rovide access to open application programming interfaces to authorized integrators" *and* "[a]dopt and make available a standardized framework for the exchange, integration and sharing of data from dealer data systems with authorized integrators and the retrieval of data by authorized integrators." A.R.S. § 28-4654(A)(1), (2). Providing access via APIs does not obviate Plaintiffs' independent obligation to create a method "for the exchange, integration and sharing of data from dealer data systems with authorized integrators and the retrieval of data by authorized integrators." And requiring Plaintiffs to enable "the exchange, integration and sharing" as well as "the retrieval of data" stored on Plaintiffs' servers cannot be reconciled with the CFAA, which grants computer owners "exclusive discretion" to determine who is authorized to access their computers. *Nosal II*, 844 F.3d at 1036; *accord Facebook*, 844 F.3d at 1063; *In re Dealer Mgmt. Sys. Antitrust Litig.*, 362 F. Supp. 3d at 570.

Finally, the CFAA would preempt the DMS Law even if —*but see infra* Section II.E (discussing GLBA)—that law did "not prevent Plaintiffs from complying with their obligations under federal law." ECF 39 at 10. Plaintiffs contend that the CFAA preempts the DMS Law because it is "an obstacle to" Congress's purpose in enacting the statute, which was to empower computer owners "to control who may access their computer systems by prohibiting hackers and others from accessing computers without the owners' authorization." Compl. ¶¶ 199, 201; *see also id.* ¶ 204. Because the DMS Law assigns a right to dealers that federal law assigns to DMS providers, "no set of circumstances exists under which the Act would be valid." *Salerno*, 481 U.S. at 745.

C. Plaintiffs' DMCA Claim Is Not Subject To Dismissal.

Defendants admit that the DMCA prohibits the "circumvention[]" of "a technological measure that effectively controls access to a [copyrighted] work." 17 U.S.C.

§ 1201(a)(1)(A); *see* ECF 39 at 10–11. And Defendants do not dispute that Plaintiffs have adopted technological measures that effectively control access to the copyrighted works residing in their DMSs. Compl. ¶¶ 8, 11, 12, 34, 39, 42, 44, 48–49, 51–68, 171–72. But, echoing their misguided CFAA arguments, Defendants contend that the DMCA does not preempt the DMS Law both because it grants access to Plaintiffs' DMSs only to third-party integrators designated by dealers, and because Plaintiffs can purportedly satisfy the law's requirements by creating APIs for third-party integrators. Both arguments fail.

According to Defendants, the DMS Law "does not authorize any circumvention of technological barriers by unauthorized parties" because "it requires DMS providers to permit data access by persons who have the dealers' written authorization to access the dealers' data." ECF 39 at 11. But that simply begs the question of who has the right to authorize access to the copyrighted materials that indisputably reside in Plaintiffs' DMSs.

Congress's intent in enacting the DMCA was to deter digital copyright infringement by amplifying "*the copyright owner's* right to control access to his or her copyrighted work." H.R. Rep. No. 105-551, pt. 2, at 38 (1998) (emphasis added). Thus, under the DMCA, unlawful "'circumvent[ion]'" of "'a technological measure'" means "to avoid, bypass, remove, deactivate, or impair a technological measure, *without the authority of the copyright owner*." 17 U.S.C. § 1201(a)(3)(A) (emphasis added). Plaintiffs allege—and Defendants do not dispute—that Plaintiffs own the copyright in various aspects of their DMSs. Compl. ¶¶ 8, 34, 42, 48–49, 62, 71, 90, 112, 144, 169–70. Accordingly, under the DMCA, it is Plaintiffs, not dealers, who have the right to control access to Plaintiffs' DMSs.[7]

None of the cases cited by Defendants, *see* ECF 39 at 11, suggest otherwise. *ITC Textile, Ltd. v. Wal-Mart Stores, Inc.*, 2009 WL 10671458 (C.D. Cal. 2009), addressed whether the DMCA applies to non-electronic dissemination of copyrighted information. It did not address who "controls access" to a protected work, much less hold that someone

[7] Notably, Defendants do not claim that dealers own any copyright in "the dealers' data." ECF 39 at 11. On the contrary, Defendants admit that "'[t]he dealer data held in the DMS is raw information … and therefore may not be copyrighted.'" *Id.* at 13 n.10.

other than the copyright owner does. Defendants cite *Ticketmaster L.L.C. v. Prestige Entm't, Inc.*, 306 F. Supp. 3d 1164 (C.D. Cal. 2018), for the proposition that "'legitimate users' that complete a CAPTCHA screen 'do not violate the DMCA.'" ECF 39 at 11. But that does not help Defendants here. As an initial matter, Plaintiffs use various technological measures, not just CAPTCHA screens, to control access to their DMSs. Compl. ¶¶ 8, 11, 12, 44, 51–68, 171–72. Regardless, *Ticketmaster* denied the defendant's motion to dismiss a DMCA claim, implicitly holding that authority for access to copyrighted material must come from the copyright owner. Referencing the defendant's use of automated bots to evade CAPTCHA controls erected by Ticketmaster to control access to its copyrighted works (*cf.* Compl. ¶¶ 56–57, 64–65, 68, 171–72), the court said that "[t]he fact that legitimate users can complete a CAPTCHA in an identical manner is irrelevant—legitimate users do so with 'the authority of [Ticketmaster]' and thus do not violate the DMCA." 306 F. Supp. 3d at 1174 (quoting 17 U.S.C. § 1201(a)(3)(A)). *Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678 (D. Md. 2011), also is of no help to Defendants. The court dismissed the plaintiffs' DMCA claim only because the plaintiffs had "not alleged any facts to suggest that [the defendant] ever accessed the [plaintiff's] website without using a security pass code issued by Plaintiffs or [their agent]." *Id.* at 692. Nothing in that case suggests that anyone other than "the copyright owner" may control access to copyrighted material.

According to Defendants, the DMS Law "reflects the Arizona Legislature's judgment that Plaintiffs' use of technological blocking to prevent dealers from allowing third parties to access their own data has … undesirable effects." ECF 39 at 11. But under the Supremacy Clause, U.S. Const. art. VI, cl. 2, it is *Congress's* judgment that governs if there is a conflict between the DMS Law and the DMCA—as there is here, given that the DMS Law eliminates Plaintiffs' exclusive control over access to its copyrighted works.

Ignoring the text of the DMCA, Defendants try to conjure policy reasons why Arizona should be allowed to ignore the DMCA's unambiguous declaration that unlawful circumvention occurs whenever anyone avoids a technological measure "without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A). Citing *MDY Industries, LLC*

v. Blizzard Entertainment, Inc., 629 F.3d 928, 951 (9th Cir. 2010), Defendants assert (ECF 39 at 12) that the Ninth Circuit has "recognize[d]" the "possibility that a party may use the 'DMCA anti-circumvention right in a manner that violates antitrust law.'" But in *MDY*, the Ninth Circuit *affirmed* the defendant's liability for a DMCA violation and the entry of a permanent injunction barring future violations. 629 F.3d at 954.[8] And far from ignoring the statutory text in favor of purported policy considerations, the court explicitly rejected the Federal Circuit's policy-motivated conclusion that actual infringement—rather than mere circumvention—is necessary to state a DMCA claim. The Ninth Circuit said that it was "unable to follow [the Federal Circuit's] approach because it is contrary to the plain language of the statute." *Id.* at 950. As it has stated before, a court's "'inquiry begins with the statutory text, and ends there as well if the text is unambiguous.'" *Amalgamated Sugar Co. LLC v. Vilsack*, 563 F.3d 822, 829 (9th Cir. 2009); *see also MDY*, 629 F.3d at 943 ("'We begin, as always, with the text of the statute.'"). As relevant here, the DMCA unambiguously "grants *copyright owners* the right to enforce th[e] prohibition" on circumvention. *MDY*, 629 F.3d at 944 (citing 17 U.S.C. § 1201(a)) (emphasis added); *id.* at 945 (characterizing 17 U.S.C. § 1201(a) as "granting copyright owners a new anti-circumvention right"). That ends the inquiry. Under the DMCA, circumventing a technological measure that protects copyrighted material is unlawful if done "without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A).

Defendants' remaining points are also meritless. The assertion that Plaintiffs can "comply with the [DMS] Law by creating an API" (ECF 39 at 12) is both wrong and irrelevant for the reasons explained above. *See supra* at 10–11. Nor is there any merit to Defendants' contention that the DMS Law survives preemption under the DMCA because it "precludes only 'unreasonable restriction[s]' on access by dealer-authorized third parties that have met STAR Standards for data security." ECF 39 at 12. In granting *dealers* the power to authorize third-party access to Plaintiffs' copyrighted material, the DMS Law is

[8] It also affirmed the denial of relief on two other DMCA claims, because the plaintiff "did not effectively control access" to the copyrighted materials at issue. 629 F.3d at 952.

in direct conflict with the DMCA, which "grants *copyright owners* the right" to control access to their copyrighted works. *MDY*, 629 F.3d at 944 (emphasis added). There is no set of circumstances under which the DMS Law can be reconciled with the DMCA.

D. Plaintiffs' Copyright Act Claim Is Not Subject To Dismissal.

Plaintiffs' DMSs contain and are comprised of copyrighted material. Compl. ¶¶ 169–170, 182. The Copyright Act gives copyright owners control over their copyrighted works. The DMS Law, by contrast, purports to give dealers and extractors a state-law right to copy and distribute copies of Plaintiffs' copyrighted works. Given this square conflict, the Copyright Act preempts the DMS Law. Nothing Defendants say suggests otherwise.

1. Using "APIs" Does Not Avoid Copyright Infringement.

Defendants argue that the Copyright Act does not preempt the DMS Law because Plaintiffs could use APIs to comply with the DMS Law without providing "access and use" of the copyrighted DMS software. ECF 39 at 13. That is wrong for at least two reasons.

First, the argument rests on disputed factual assertions that cannot be resolved on a motion to dismiss. Defendants assert that use of an API "would not require access to the DMS," ECF 39 at 13, but Plaintiffs allege that "[i]t is impossible … to access or use the Reynolds DMS without running (and thereby copying) Reynolds's copyrighted … software" and that such access "necessarily entails the display, distribution, and creation of copies and derivative works of the copyrighted DMS software." Compl. ¶¶ 49, 183; *see also A Dictionary of Computing* 19 (6th ed. 2008) (an API is "a set of functions and procedures [that] enables a program to gain access to facilities within an application"). Plaintiffs' allegations must be treated as true at this stage of the proceedings. *Ortega Melendres v. Arpaio*, 598 F. Supp. 2d 1025, 1035 n.3 (D. Ariz. 2009).

Second, APIs themselves are (or would be) part of Plaintiffs' copyrighted works. *See Oracle Am., Inc. v. Google Inc.*, 750 F.3d 1339, 1381 (Fed. Cir. 2014) ("API packages … are entitled to copyright protection."). Even if Plaintiffs could be compelled to create APIs for the DMS software—which they cannot (*see* Compl. ¶¶ 248–54)—giving dealers and integrators a state-law right to copy and distribute such APIs conflicts with the exclusive

rights that Plaintiffs would hold for those APIs under the Copyright Act.

2. Allowing Parties To Exploit Plaintiffs' Software Is Not "Fair Use."

Defendants argue, ECF 39 at 14, that the Copyright Act cannot preempt the DMS Law because it is, supposedly, consistent with the Copyright Act's "fair use" provision, 17 U.S.C. § 107. This theory does not withstand scrutiny.

To start, the premise of Defendants' "fair use" argument—that creating unauthorized copies of Plaintiffs' copyrighted work is "necessary for dealers to gain access to their own data," ECF 39 at 14—is contrary to the well-pleaded allegations of the Complaint, according to which licensed dealers are able to access the data in the DMS systems and transfer it to whomever they please. Compl. ¶¶ 42, 100, 101, 107. Those allegations must be accepted as true. *Ortega*, 598 F. Supp. 2d at 1035 n.3. Moreover, to the extent dealers input data into the DMS, they necessarily have original access to that data.

Defendants also fail to even cite—much less discuss—the statutory "fair use" factors:

> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.

17 U.S.C. § 107. Defendants' silence is likely strategic as these factors are fact-dependent and generally cannot be resolved on a motion to dismiss. *Browne v. McCain*, 611 F. Supp. 2d 1073, 1078 (C.D. Cal. 2009) ("[C]ourts rarely analyze fair use on a 12(b)(6) motion").

Here, the Complaint's well-pleaded factual allegations foreclose dismissal of Plaintiffs' Copyright Act claim on "fair use" grounds. The Complaint alleges: that dealers and their third-party integrators use Plaintiffs' copyrighted works for commercial purposes, Compl. ¶¶ 2, 3; that those works include software code which Plaintiffs have invested hundreds of millions of dollars to develop, *id.* ¶¶ 13, 27, 34, 39, 47; that access to Plaintiffs' DMSs as required by the DMS Law will necessarily include "the display, distribution, and creation of copies and derivative works of the copyrighted DMS software," *id.* ¶ 183; and that the impact of the DMS Law on the value of Plaintiffs' systems will be staggering

because dealers will no longer need to compensate Plaintiffs for use of their software, *id.* ¶¶ 34, 95, 108, 132, because the demands of the DMS Law would degrade the performance of Plaintiffs' DMSs, *id.* ¶¶ 116–19, and because access under the DMS Law would also introduce significant security risks, *id.* ¶¶ 120–25. Thus, contrary to Defendants' assertion, ECF 39 at 14, the DMS law does not come close to "textbook fair use."

3. The Copyright Act And DMS Law Do Not Share A Common Purpose.

Defendants also argue that Plaintiffs' claim under the Copyright Act should be dismissed because the DMS Law purportedly "shares the Act's" supposed goal of preventing "copyright misuse." ECF 39 at 14–15. There is no merit to that argument.

As an initial matter, the DMS law is not directed to curbing the misuse of copyrights. Plaintiffs and other DMS providers have invested hundreds of millions of dollars in developing their copyrighted works. Compl. ¶¶ 13, 27, 34, 39, 47. Exercising the exclusive rights granted them under the Copyright Act to protect those works from infringement is the antithesis of copyright misuse.

Moreover, while copyright "misuse" might be "an equitable defense" to an infringement action, *Omega S.A. v. Costco Wholesale Corp.*, 776 F.3d 692, 699 (9th Cir. 2015) (Wardlaw, J., concurring), Defendants do not cite—and Plaintiffs are not aware of—any authority suggesting that one of Congress's objectives in enacting the Copyright Act was to prevent such misuse. In fact, "[c]opyright misuse is a *judicially* crafted affirmative defense." *Apple Inc. v. Psystar Corp.*, 658 F.3d 1150, 1157 (9th Cir. 2011) (emphasis added). And even if Congress had sought to prevent copyright misuse, that would not save the DMS Law from preemption given that its method of achieving that purported aim—vesting dealers with rights that the Copyright Act assigns exclusively to Plaintiffs as copyright owners—squarely conflicts with federal law. Regardless, because copyright misuse is an affirmative defense that does not appear on the face of the complaint, Defendants bear the burden of presenting evidence to sustain it. *Cf. Michael Grecco Prods., Inc. v. Valuewalk, LLC*, 345 F. Supp. 3d 482, 504 (S.D.N.Y. 2018). They have not done so and may not do so

at this stage of the proceedings. *Hal Roach Studios, Inc. v. Richard Feiner & Co.*, 896 F.2d 1542, 1555 n.19 (9th Cir. 1989).

E. Plaintiffs' GLBA Claim Is Not Subject To Dismissal.

Defendants argue that Plaintiffs' GLBA claim fails because "Plaintiffs do not allege that the GLBA applies to CDK and Reynolds—only that *dealers* are 'financial institutions' subject to the GLBA's regulations." ECF 39 at 16. But that is not fatal to the claim.[9]

As an initial matter, the FTC takes the position that "*[s]ervice providers* are accountable for protecting the personal data they collect and store" and "may be liable for violations of the [GLBA]." Lesley Fair, *Data Security Settlement with Service Provider Includes Updated Order Provisions*, FTC BUSINESS BLOG (June 12, 2019) (emphasis added), https://www.ftc.gov/news-events/blogs/business-blog/2019/06/data-security-settlement-service-provider-includes-updated. Plaintiffs allege that they are "service providers" within the meaning of the GLBA. Compl. ¶¶ 81–82, 89, 94, 212. Thus, Plaintiffs' failure to allege that they are "financial institutions" under the GLBA is immaterial.

Moreover, the theory propounded in the Complaint is that the DMS Law prevents dealers from fulfilling their obligations under the GLBA by preventing Plaintiffs, the dealers' service providers, from adequately securing the data they store. Defendants denigrate this theory as "novel" (ECF 39 at 17), but novelty is not a defense, especially when the DMS Law is one of the first of its kind. *Cf.* ECF 39 at 4 (citing other DMS laws, but none enacted before 2019). Defendants also do not explain why the DMS Law would survive preemption under the GLBA merely because it prevents dealers, rather than DMS providers, from fulfilling duties imposed by the GLBA.[10] Either way, there is a conflict between the

[9] The Federal Trade Commission—one of the agencies responsible for implementing the GLBA—has recently alleged that a DMS provider is a "financial institution" within the meaning of the GLBA. *In re Lightyear Dealer Techs. LLC*, F.T.C. Complaint ¶ 23, https://www.ftc.gov/system/files/documents/cases/172_3051_dealerbuilt_final_complaint_6-12-19.pdf.

[10] Disregarding the Complaint's well-pleaded allegations (*e.g.* Compl. ¶¶ 213–16), Defendants suggest that the restrictions placed on DMS providers by the DMS Law do not interfere with the fulfillment of dealers' obligations under the GLBA. *Cf.* ECF 39 at 17. But, on a motion to dismiss, the Complaint's well-pleaded allegations must be accepted as true. *Ortega*, 598 F. Supp. 2d at 1035 n.3.

two statutes and, under the Supremacy Clause, the DMS Law must yield.

F. Plaintiffs' DTSA Claim Is Not Subject To Dismissal.

Defendants argue that Plaintiffs' DTSA claim fails for two reasons. Neither argument has merit.

First, Defendants assert that acquisition of a trade secret is prohibited by the DTSA only if the acquisition is by "'improper means,'" a term defined to exclude "'lawful means of acquisition.'" ECF 39 at 15 (quoting 18 U.S.C. §§ 1839(5), (6)).[11] From this, Defendants conclude that the DMS Law "poses no conflict with the DTSA" because the DMS Law "simply specifies a 'lawful means' through which dealer-authorized third parties may access dealer data." *Id.* But that assertion assumes that a state legislature may, notwithstanding the Supremacy Clause, deprive trade-secret owners of their federal right to control access to their trade secrets. Defendants do not cite—and Plaintiffs are not aware of—any authority for that proposition.[12]

Federal law gives the owners of trade secrets the right to control access to those secrets. Federal law makes it a crime for anyone to "appropriate[]," "cop[y]," "upload," or "transmit[]" a trade secret "without authorization" for "the economic benefit of anyone other than the owner thereof." 18 U.S.C. § 1832(a). Trade-secret owners also enjoy the right to enforce that prohibition through a "civil action." *Id.* § 1836(b)(1). It would materially

---

[11] Not all violations of the DTSA require "improper means." It also prohibits "use of a trade secret of another without express or implied consent by a person who[,] … at the time of … use, knew or had reason to know that the knowledge of the trade secret was … derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret." 18 U.S.C. § 1839(5)(B)(ii)(III). This section does not use the term "improper means" and thus does not exclude the use of trade secrets acquired by "other lawful means," *id.* § 1839(6)(B), from its scope. So if a third-party integrator gains access to the trade secrets in Plaintiffs' DMSs from a dealer exercising its rights under the DMS Law and the integrator knows or has reason to know that the dealer is contractually obligated to maintain the secrecy of those trade secrets (*cf.* Compl. ¶¶ 86, 90), the third-party integrator has violated the DTSA.

[12] Construing the phrase "other lawful means of acquisition," 18 U.S.C. § 1839(6)(B), to include state-authorized access over an owner's objection would create a conflict between § 1839(6)(B) and § 1839(6)(A), which defines "improper means" to include the "breach of a duty to maintain secrecy." Plaintiffs' contracts with dealers obligate dealers to maintain the secrecy of Plaintiffs' trade secrets. Compl. ¶¶ 86, 90, 92. If state law could declare such contractual duties of secrecy void, as the DMS Law effectively does, it would render the breach-of-duty provision in § 1839(6)(A) meaningless.

weaken that federally conferred right if states could adopt laws that, like the DMS Law, compel trade-secret owners to disclose their secrets. Indeed, "the right to exclude others is central to the very definition" of a trade secret. *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1011 (1984). By forcing DMS providers to abandon the "reasonable measures" they have taken "to keep such information secret," 18 U.S.C. § 1839(3)(A), the DMS Law "stands as an obstacle" to Congress's goal of empowering trade secret owners, *Hines*, 312 U.S. at 67. The DTSA therefore impliedly preempts the DMS Law.

Second, Defendants argue that Plaintiffs "have not plausibly alleged that any trade secrets will be stolen" if the DMS Law "is enforced." ECF 39 at 15. But as Defendants admit (*id.* at 15–16), Plaintiffs have pleaded that their DMSs "contain[] numerous … trade secrets, including … forms, accounting rules, tax tables, and proprietary tools and data compilations." Compl. ¶¶ 191–92. Defendants say that is irrelevant because the DMS Law "only allows access to Protected Dealer Data as specifically defined in the statute, not any of these alleged trade secrets." ECF 39 at 16. Yet that assertion ignores the statute's sweeping definition of "protected dealer data" (*see supra* at 3) and is contrary to the Complaint's well-pleaded allegation that, because "DMSs house both 'protected dealer data' as defined by the DMS Law and other proprietary data, including Plaintiffs' intellectual property," the DMS Law's ban on "'tak[ing] any action by contract, technical means or otherwise to prohibit or limit a dealer's ability to protect, store, copy, share or use protected dealer data'" effectively "grants third parties access to that other proprietary data as well." Compl. ¶ 111 (quoting A.R.S. § 28-4653(A)(3)). The Complaint also alleges that "every time a hostile third party accesses a Plaintiff DMS using dealer-provided login credentials, that third party uses valuable CDK or Reynolds intellectual property, including patented and copyrighted technologies and original software elements and programs." *Id.* ¶ 112. It further alleges that "when third-party data extractors access the DMSs, they create a copy of portions of the DMS program code—as well as copies of the original and distinctive page layouts, graphical content, text, arrangement, organization, display of information, and dynamic user experience—in the Random Access Memory of the extractor's computer." *Id.* ¶ 113.

And it alleges that "[e]ven when third-party data extractors do not access proprietary data directly, they often access and copy data created using CDK or Reynolds and third-party proprietary forms and functions within the DMS." *Id.* ¶¶ 112–13.

These allegations are more than sufficient to plead a DTSA violation. Indeed, another court denied an integrator's motion to dismiss a DTSA claim premised on essentially identical allegations. There, as here, "CDK allege[d] that its 'DMS contains numerous proprietary CDK trade secrets, including forms, accounting rules, tax tables, and proprietary tools and data 'compilations'" and that an integrator accessing the DMS without CDK's authorization constituted misappropriation under the DTSA. *In re Dealer Mgmt. Sys. Antitrust Litig.*, 362 F. Supp. 3d at 573–74. "These allegations," the court held, "suffice at the motion to dismiss stage." *Id.* at 574. Notably, the court *rejected* the argument, advanced by Defendants here, that CDK's DTSA claim "should be dismissed because [the third-party integrator] only accesses dealer data." *Id.*; *cf.* ECF 39 at 16. That argument failed, the court held, because, as in this case, CDK had alleged that access to the DMS resulted in unauthorized access to CDK "'forms, accounting rules, tax tables, and proprietary tools and data compilations.'" *In re Dealer Mgmt. Sys. Antitrust Litig.*, 362 F. Supp. 3d at 574; *cf.* Compl. ¶¶ 191–92. Thus, Plaintiffs have stated a claim under the DTSA.

III. Plaintiffs' Constitutional Claims Are Not Subject To Dismissal.

A. The Complaint States A Void-For-Vagueness Claim.

Plaintiffs allege that the DMS Law is unconstitutionally vague because it is internally contradictory and fails to place Plaintiffs on notice as to what conduct is prohibited, while imposing criminal penalties for violations. Compl. ¶¶ 21, 145–58, 218–25. In response, Defendants argue that: (1) the DMS Law is not subject to a facial challenge for vagueness because it does not implicate First Amendment interests; (2) the DMS Law cannot be subject to an as-applied challenge because it has yet to be applied; (3) certain terms used in the DMS Law are sufficiently defined or not subject to challenge; and (4) any ambiguities in the DMS Law can be resolved through incremental judicial interpretation. ECF 40 at 13–14. None of these arguments provides a basis for dismissal.

Defendants' first argument is inaccurate. To start, the Complaint alleges that the DMS Law implicates First Amendment interests. Compl. ¶¶ 249–54. In addition, statutes not implicating the First Amendment are still subject to facial vagueness challenges. *See, e.g., Guerrero v. Whitaker*, 908 F.3d 541, 544 (9th Cir. 2018); *Humanitarian Law Project v. U.S. Treasury Dep't*, 578 F.3d 1133, 1146 (9th Cir. 2009); *Hotel & Motel Ass'n of Oakland v. City of Oakland*, 344 F.3d 959, 971 (9th Cir. 2003).

Second, even if Plaintiffs were limited to an as-applied challenge, such challenges need not always await actual enforcement by the State. The one case Defendants cite for this proposition, *Hoye v. City of Oakland*, 653 F.3d 835, 859 (9th Cir. 2011), did not state a categorical rule, holding only that the as-applied challenge *in that case* was fact-intensive, requiring too much speculation "as to prospective facts" because it was unclear (due to the parties' litigation history) how Oakland would enforce its challenged ordinance against the plaintiff. Here, the Court is not called upon to speculate about prospective facts in addressing Plaintiffs' claims. Further, courts routinely consider pre-enforcement as-applied constitutional challenges. *See Isaacson v. Horne*, 716 F.3d 1213, 1230 n.15 (9th Cir. 2013).

Third, Defendants argue that the terms "fee" and "dealer data" are not vague because they "have specific definitions and give clear notice regarding their meanings." ECF 40 at 13. This argument ignores the allegations that the definition of "fee" is unclear (Compl. ¶¶ 149–51, 224(d)) and that because of the interplay between the statutory provisions, Plaintiffs are uncertain what "dealer data" is covered by the law (*id.* ¶¶ 148, 153–55, 224(f)). Defendants offer no response to these allegations.

Defendants attempt to cure the DMS Law's ambiguity by offering their own interpretation of some (but not all) challenged terms in the statute. ECF 40 at 14. But courts have "expressly rejected the notion that a statutory provision survives a facial vagueness challenge merely because *some* conduct clearly falls within the statute's scope." *Guerrero*, 908 F.3d at 544 (emphasis added). Defendants also argue that the word "unreasonable" is not unconstitutionally vague "as a matter of law." ECF 40 at 13. That is not true. *See, e.g., St. Mark Roman Catholic Par. Phoenix v. City of Phoenix*, 2010 WL 11519169, at *8 (D.

Ariz. 2010) (plaintiffs stated plausible claim that words such as "unreasonably loud" and "unnecessary" required guessing as to scope and meaning). The question is whether the statute "fails to give ordinary people fair notice of the conduct it punishes, or so standardless that it invites arbitrary enforcement." *Guerrero*, 908 F.3d at 543. Plaintiffs sufficiently allege that, *inter alia*, the DMS Law leaves reasonable data vendors to guess as to which restrictions are permissible or "unreasonable." Compl. ¶¶ 131, 152, 224(e).

Finally, judicial interpretation taking place years from now will not cure the law's defects in the present, and, as Plaintiffs allege, their current business operations will suffer significantly due to the uncertainty caused by the DMS Law. Indeed, in conceding that such exposition may be needed, Defendants implicitly concede that the law is vague as drafted.

B. The Complaint States A Takings Claim.

The Complaint states a compelling claim that the DMS Law violates the Constitution's Takings Clause. Defendants do not, and cannot, dispute that Plaintiffs have a significant property interest in their proprietary DMSs. *See generally Ruckelshaus*, 467 U.S. at 1001, 1003–04 (recognizing that takings analysis applies to intangible property and commercial data such as trade secrets); *see also CCC Info. Servs., Inc. v. Maclean Hunter Mkt. Reports, Inc.*, 44 F.3d 61, 74 (2d Cir. 1994) (depriving copyright owner of its property "would raise very substantial problems under the Takings Clause of the Constitution"). And Plaintiffs further allege that the taking here is not for a public purpose, but rather to serve dealers' private economic interests. Compl. ¶ 230; *see Kelo v. City of New London, Conn.*, 545 U.S. 469, 478 (2005). A "taking must be for a 'public use,'" *Brown v. Legal Found. of Wash.*, 538 U.S. 216, 231 (2003), and "[a] court confronted with a plausible accusation of impermissible favoritism to private parties should treat the objection as a serious one and review the record to see if it has merit[.]" *Kelo*, 545 U.S at 491 (Kennedy, J. concurring). And even if there were a public purpose behind the taking, the DMS Law fails to provide just compensation. Compl. ¶ 232.

Defendants first argue that the DMS Law does not require Plaintiffs to allow third parties to access their proprietary DMSs, so nothing is taken from them. ECF 40 at 9. This

ignores the well-pleaded allegations that the law requires Plaintiffs to open access to their systems. Compl. ¶ 14, 19, 131–42. Further, building and maintaining open APIs to process requests from external third parties requires Plaintiffs to create intellectual property, devote system resources, and incur real expense to enable unlicensed third parties to leverage their propriety system and software (including the new APIs themselves). That would be contrary to Plaintiffs' ownership rights in their systems and license agreements with dealers.

Defendants next argue that Plaintiffs have no proprietary rights in the dealer data that is "removed" from the DMSs because that data "belongs to the dealers." ECF 40 at 9. But this ignores the allegation that the DMSs contain "both 'protected dealer data' as defined by the DMS Law *and other proprietary data, including Plaintiffs' intellectual property* and data licensed to Plaintiffs by OEMs and other parties." Compl. ¶ 111 (emphasis added). Moreover, the DMS Law requires Plaintiffs to allow third parties to use the hardware and software components of the DMSs, such as "valuable intellectual property including patented technologies, proprietary software elements and programs (including software programs eligible for protection by the copyright laws), and proprietary data collections." *Id*. ¶¶ 39, 47–48.

Defendants also argue that there is no physical taking of Plaintiffs' property. ECF 40 at 9. But Plaintiffs allege that the DMS Law is a *per se* taking because the "interference" with Plaintiffs' property amounts to "a physical invasion by government," *Penn Central Transp. Co. v. City of New York*, 438 U.S. 104, 124 (1978)—the "functional equivalent of a 'practical ouster of [the owner's] possession,'" *Lingle v. Chevron U.S.A., Inc.*, 544 U.S. 528, 537 (2005). No one can access Plaintiffs' DMSs without occupying Plaintiffs' hardware and using their intellectual property. Compl. ¶¶ 39, 49, 112. The DMS Law also permits third parties to "write" data to a DMS, altering the content of the DMS itself. *See* A.R.S. § 28-4653(A)(3)(a), (b). By permitting third parties to use Plaintiffs' hardware and software to access and rewrite their DMSs without Plaintiffs' permission, the DMS Law "requires [Plaintiffs] to suffer a permanent physical invasion of [their] property," *Lingle*, 544 U.S. at 538, a *per se* taking.

Plaintiffs also plead a regulatory taking. In *Penn Central*, the Supreme Court emphasized that the regulatory-taking test is "essentially [an] ad hoc, factual inquir[y]." 438 U.S. at 124. Among the relevant factors are "the character of the governmental action, its economic impact, and its interference with reasonable investment-backed expectations." *Ruckelshaus*, 467 U.S. at 1005. Such a "factual inquiry" is not suited to resolution on a motion to dismiss.

The Complaint alleges that the DMS Law will have a significant economic impact on Plaintiffs and substantially interfere with their reasonable investment-backed expectations. Plaintiffs have invested heavily to maintain and enhance their proprietary systems. Compl. ¶¶ 39, 47. They protect their investment by making their DMSs available only through "contracts [that] contain detailed provisions setting forth Plaintiffs' exclusive rights to control third-party access to their proprietary DMS systems." *Id.* ¶ 84. Plaintiffs charge fees to authorized users to recoup their investment in the DMSs and to compensate them for the value of their services and the intellectual property that makes secure data integration with Plaintiffs' DMSs possible. *Id.* ¶ 99.

The DMS Law undercuts Plaintiffs' extensive efforts to protect the confidentiality, integrity, and availability of their DMSs. *Id.* ¶¶ 127, 143. The very purpose of the DMS Law is to permanently deprive Plaintiffs of their property by granting unfettered use to unlicensed third parties.[13] *Id.* ¶ 132. The allegations thus establish that the DMS Law effects a regulatory taking of Plaintiffs' intellectual property.

Finally, Defendants claim that the DMS Law does not deprive Plaintiffs of just compensation because the law allows Plaintiffs to recover certain "direct costs." ECF 40 at 10. But just compensation "is to be measured by 'the *market value* of the property at the time of the taking.'" *Horne v. Dep't of Agric.*, 135 S. Ct. 2419, 2432 (2015) (emphasis added). The market value of Plaintiffs' DMSs is not simply the direct cost of providing access to someone who does not have Plaintiffs' permission to use their property but the

[13] *See Dolan v. City of Tigard*, 512 U.S. 374, 394 (1995) (permanent easement eviscerates right to exclude because plaintiff would lose right to regulate when the public could enter the property).

value to unlicensed parties of the access they seek. That value is the negotiated market rate that Plaintiffs would receive in exchange for the right to use the DMS, not merely direct costs. The DMS Law strips Plaintiffs of the market value of their property.

C. Plaintiffs' Contracts Clause Claim Is Not Subject To Dismissal.

Under the Contracts Clause, laws changing the enforceability of contract provisions are subjected to a two-part test. *Pure Wafer, Inc. v. City of Prescott*, 845 F.3d 943, 952 (9th Cir. 2017). First, the Court examines "whether the state law has operated as a substantial impairment of a contractual relationship." *Sveen v. Melin*, 138 S. Ct. 1815, 1821–22 (2018) (internal quotation marks omitted). If so, the Court then determines "whether the state law is drawn in an appropriate and reasonable way to advance a significant and legitimate public purpose." *Id*. at 1822 (internal quotation marks omitted). "[T]he level of scrutiny to which the legislation will be subjected" increases as "[t]he severity of the impairment" does. *Energy Reserves Grp., Inc. v. Kan. Power & Light Co.*, 459 U.S. 400, 411 (1983).

With regard to the first step, Defendants do not suggest that Plaintiffs fail to adequately allege a contractual relationship, an impairment of that relationship, or that the impairment is substantial. ECF 40 at 7–8. Instead, they argue that Plaintiffs did not adequately plead a facial challenge to the DMS Law because they did not allege how the law will impair *future* contracts. *Id*. at 7. This is a non-sequitur because the Complaint focuses on Plaintiffs' *existing* contractual relationships with Arizona car dealerships, without purporting to allege an impairment of future contracts. Compl. ¶¶ 85, 90. A claim that a law impairs pre-existing contracts plainly falls within the scope of the Contracts Clause. *See Sveen*, 138 S. Ct. at 1821.

Regarding the second step of the test, Plaintiffs cite two out-of-circuit district court cases to argue that courts "routinely dismiss Contracts Clause claims where—as here—the legislature had a legitimate objective in enacting the legislation at issue." ECF 40 at 8. But this misstates the applicable test. The level of scrutiny depends on the severity of the impairment. *Energy Reserves Grp.*, 459 U.S. at 411. Here, Plaintiffs have alleged (and Defendants do not contest) that the DMS Law substantially impairs their contractual

relationships with dealers in three significant ways: (1) it overrides contractual provisions prohibiting dealers from granting third parties access to the DMSs without Plaintiffs' prior authorization (Compl. ¶¶ 131–33, 237); (2) it prevents Plaintiffs from complying with their contractual obligations to safeguard the security of the data in the DMS (*id.* ¶¶ 138, 142, 239); and (3) it impairs Plaintiffs' contractual relationships with dealers by imposing a 90-day termination clause on the contracts (*id.* ¶¶ 139, 238). Given the importance of these provisions to the contractual relationship, the extent of the impairment is great and the level of scrutiny is correspondingly higher. *See Energy Reserves Grp.*, 459 U.S. at 411.

Nor have Plaintiffs conceded the existence of a legitimate public purpose for the DMS Law, as Defendants contend. ECF 40 at 8. To the contrary, Plaintiffs allege that the Law's purpose was to provide an economic benefit to a narrow class of private actors—the car dealers. Compl. ¶¶ 2–3, 143, 240. A law that exhibits a "bald preference for one class of contracting citizens over another … suggest[s] the kind of favored treatment that clearly exceeds the state's police power," *Ross v. City of Berkeley*, 655 F. Supp. 820, 833 (N.D. Cal. 1987), and because the DMS Law "affects only [a] narrow class" of economic actors, it does not serve a legitimate public purpose, *Cycle Barn, Inc. v. Arctic Cat Sales, Inc.*, 701 F. Supp. 2d 1197, 1203–04 (W.D. Wash. 2010). Defendants seize on what they claim to be an admission in the complaint that the DMS Law is a cybersecurity measure meant to protect consumers. ECF 40 at 8 (citing Compl. ¶ 126). But Plaintiffs allege that this description of the DMS Law *misstates* the law's true purpose. Compl. ¶¶ 2, 126, 143.

And even if there were a legitimate purpose to the DMS Law, that does not end the inquiry. The law still must be "drawn in an appropriate and reasonable way to advance" the "significant and legitimate" public purpose. *Sveen*, 138 S. Ct. at 1822. Defendants ignore the "appropriate and reasonable" requirement. And Plaintiffs have adequately pleaded that the DMS Law is not an appropriate and reasonable means of serving any legitimate interest because, for instance, its true purpose is to rewrite the contractual relationships of private parties, and it places consumer data at risk to provide an economic benefit to car dealers. *See, e.g.*, Compl. ¶¶ 142–43, 240.

D. The Complaint States A Dormant Commerce Clause Claim.

Defendants contend that Plaintiffs "do not—and cannot—allege that the DMS Law discriminates against interstate commerce," ECF 40 at 15, but the Commerce Clause prohibits states from directly *regulating* interstate commerce, *Shafer v. Farmers Grain Co.*, 268 U.S. 189, 199 (1925). Here, Plaintiffs' DMSs operate nationwide but Arizona has placed special rules on how they must operate. "[S]ignificant burdens on interstate commerce generally result from inconsistent regulations of activities that are inherently national or require a uniform system of regulation." *Nat'l Ass'n of Optometrists & Opticians v. Harris*, 682 F.3d 1144, 1148 (9th Cir. 2012).

A state law may regulate interstate commerce only if the statute serves a legitimate public interest, the effect on interstate commerce is incidental, and the burden on interstate commerce is not "clearly excessive in relation to the putative local benefits." *Pike v. Bruce Church, Inc.*, 397 U.S. 137, 142 (1970). This balancing test is fact-intensive and ill-suited to resolution on a motion to dismiss. *See Magna Legal Servs. v. Ariz. ex rel. Bd. of Certified Reporters*, 2013 WL 4478933, at *7 (D. Ariz. 2013). Regardless, Plaintiffs satisfy it.

First, the Complaint alleges that the DMS Law does not serve a legitimate public interest because it rewrites private contracts, puts consumer data at risk, and exposes DMS providers to cyberattacks that could threaten *all* DMS operations, including interstate commerce unrelated to any transaction in Arizona. Compl. ¶¶ 6–8, 132–33, 142.

Second, the Complaint alleges that the DMS Law burdens interstate commerce by directly and substantially interfering with Plaintiffs' interstate operations. By necessity DMSs operate on a national scale, operate across state lines, and are not designed to accommodate individual state requirements. *Id.* ¶ 35. Additionally, unfettered third-party access to the DMSs risks system degradation nationwide. *Id.* ¶¶ 116, 119, 143.

Finally, the law is unnecessary to achieve its purported purpose of facilitating DMS interoperability with third parties because Plaintiffs already provide multiple ways to allow third parties to securely interoperate with the DMSs and/or receive the data vendors require to render services to dealers. *See id.* ¶¶ 96–107. The practical effect of the DMS Law is not

to serve public interests, but to regulate Plaintiffs' interstate operations at great risk to dealers and consumers. This states a claim.

E. The Complaint States A First Amendment Claim.

Defendants admit that Plaintiffs will be compelled to write computer code if the DMS Law goes into effect. ECF 40 at 11; *see* ECF 39 at 4; *see also* Compl. ¶¶ 19, 249–52. Thus, if the First Amendment applies, Plaintiffs state a cause of action because "[m]andating speech that a speaker would not otherwise make necessarily alters the content of the speech" and thus demands "exacting First Amendment scrutiny." *Riley v. Nat'l Fed'n of the Blind of N. Carolina, Inc.*, 487 U.S. 781, 795, 798 (1988). For their part, Defendants do not contend that the DMS Law serves a compelling interest or is narrowly tailored.

Instead, Defendants contend that the DMS Law is not subject to First Amendment scrutiny because (1) the law does not compel Plaintiffs to "share" information with third parties and (2) the law regulates conduct, not speech. ECF 40 at 10–12. Neither argument has merit. First, Plaintiffs are not merely conduits facilitating the transmission of information between dealers and third-party integrators, as Defendants contend. Rather, Plaintiffs organize information belonging to dealers and others in their proprietary DMSs, and the DMS Law requires them to share that information, as they have organized it, with third parties. Compl. ¶¶ 131–42. Further, by requiring Plaintiffs to allow integrators to interact with Plaintiffs' proprietary systems, Plaintiffs are compelled to communicate with third parties, not merely pass others' information along. *Id.* ¶ 214.

Second, the computer code Plaintiffs must write falls within the First Amendment's protection, so the DMS Law necessarily regulates speech. *See, e.g.*, *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449 (2d Cir. 2001); *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000). As one court noted, "[C]omputer language is just that, language, and it communicates information either to a computer or to those who can read it." *Bernstein v. Dep't of State*, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996). Source code is inherently expressive as a "means for the exchange of information and ideas about computer programming," *Junger*, 209 F.3d at 485, and because it communicates information to end-

users, *Corley*, 273 F.3d at 448.

Defendants assert that the law regulates conduct, not speech, because it "simply requires that a market product (Plaintiffs' DMS) has certain functionality (the ability to allow dealers to access and share their own data)." ECF 40 at 12. But that required "functionality" forces Plaintiffs to speak by writing computer code. And this alteration to Plaintiffs' system is hardly incidental; it is the DMS Law's very purpose. Dealers already have the ability to share their data stored in the DMS with third parties, free of charge. Compl. ¶¶ 42, 100–01, 107. Unhappy with that, the dealers orchestrated this law to provide different means of sharing their information by effectively opening up Plaintiffs' systems. *Id.* ¶¶ 2–3, 143, 240. This new access can only be effectuated by writing new code, so the speech aspect of the law is at its core.

Defendants' argument that there is no problem because "Plaintiffs may draft the code however they want," misses the point. ECF 40 at 11. The compulsion is in requiring Plaintiffs to change their code, even if the law does not dictate explicitly how they must do so. That is no different than requiring a party to support a cause without specifying the particular words of support. Finally, Defendants' argument (*see* ECF 40 at 12) that it is "extremely unlikely that anyone could understand Plaintiffs to be expressing any message whatsoever" misses the mark. At a minimum, any code Plaintiffs draft would communicate "ideas about computer programming[,]" *Junger*, 209 F.3d at 485, "either to a computer or to those who can read it[,]" *Bernstein*, 922 F. Supp. at 1435.

CONCLUSION

For the foregoing reasons, the Court should deny Defendants' motions to dismiss.

RESPECTFULLY SUBMITTED this 18th day of October, 2019.

QUARLES & BRADY LLP
Renaissance One
Two North Central Avenue
Phoenix, AZ 85004-2391

By */s/ Brian A. Howie*
Brian A. Howie
Lauren Elliott Stine
Attorneys for Plaintiffs

SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
2099 Pennsylvania Ave., NW, Ste. 100
Washington, DC 20006, 201-747-1900
Thomas J. Dillickrath* (DC 483710)
TDillickrath@sheppardmullin.com

Four Embarcadero Center, 17th Floor
San Francisco, CA 94111, 415-434-9100
Amar S. Naik* (CA 307208)
ANaik@sheppardmullin.com
Molly C. Lorenzi* (CA 315147)
MLorenzi@sheppardmullin.com

GIBBS & BRUNS LLP
1100 Louisiana, Ste. 5300
Houston, TX 77002, 713-650-8805
Aundrea K. Gulley* (TX 24034468)
agulley@gibbsbruns.com
Denise Drake* (TX 24092358)
DDrake@gibbsbruns.com

Attorneys for The Reynolds and Reynolds Company

MAYER BROWN LLP
71 S. Wacker Drive
Chicago, IL 60606
312-782-0600
Britt M. Miller* (IL 6256398)
BMiller@mayerbrown.com
Michael A. Scodro* (IL 6243845)
MScodro@mayerbrown.com
Brett E. Legner* (IL 6256268)
BLegner@mayerbrown.com

1999 K Street, NW
Washington, DC 20006
202-263-3000
Mark W. Ryan** (DC 359098)
mryan@mayerbrown.com
Andrew E. Tauber** (DC 495980)
atauber@mayerbrown.com

Attorneys for CDK Global, LLC

**Admitted Pro Hac Vice*
***Pro Hac Vice Forthcoming*